FAST NIELSEN-THURSTON CLASSIFICATION OF BRAIDS

MATTHIEU CALVEZ

ABSTRACT. We prove the existence of an algorithm which solves the reducibility problem in braid groups and runs in cubic time with respect to the braid length for any fixed braid index.

1. Introduction and statements of the main results

One of the main algorithmic decision problems regarding braids is the problem to determine the Nielsen-Thurston type of a given braid: reducible, periodic or pseudo-Anosov [18],[12],[17]. This problem is called the *reducibility* problem because it amounts to determining whether a given non-periodic braid is reducible or not, i.e. whether it is reducible or pseudo-Anosov. Indeed, the case of periodic braids can be easily discarded: a braid x is periodic if and only if its nth power or its $(n-1)$st power is a power of the half-twist Δ (see [6]); and this is easy to decide algorithmically.

To solve the reducibility problem, two kinds of techniques were used and several algorithms were written; however none of them works in polynomial time with respect to the braid length for the general braid group B_n.

Firstly, the Bestvina-Handel algorithm [3] uses the theory of train-tracks and it is valid for any mapping class group. Although this algorithm works fast in practice, its theoretical complexity remains unknown.

Secondly, connections between the reducibility problem and the Garside structures of braid groups have also been used for detecting reducibility (see [14] for the definition of a Garside group, see [19], [15], [20] for an introduction to the classical Garside structure of B_n, and [7] for the dual structure).

Benardete, Gutierrez and Nitecki initiated the Garside-theoretical approach in [1] and [2]. Using the classical Garside structure, they showed that the reducibility of a braid x is detectable if one knows all the elements of the super summit set of x. Indeed, it suffices to check whether some element of the super summit set preserves a family of *round* curves. The same can be done with the dual Garside structure and *standard* curves replacing round curves [9]. Unfortunately, both algorithms are exponential because they demand computing the whole super summit sets, which in both structures have in general exponential size with respect to both braid length and braid index (see [26], [22]).

2010 *Mathematics Subject Classification.* 20F36, 20F10, 20F65.

The author's doctoral studies are supported by a grant ARED from Région Bretagne. This work was also partially supported by the Spanish Project MTM2010-19355.

In [24], Lee and Lee replaced the above condition about *some* element of the *super* summit set of a reducible braid x by the condition that *every* element of the *ultra* summit set of x preserves a family of round curves. However this was shown at the cost of a technical hypothesis about the external and internal components of x.

In the special case of the four-strand braid group B_4, a polynomial-time algorithm for solving the reducibility problem was constructed in [11]. This is achieved by showing that every element of the (classical) super summit set of a given reducible 4-braid with a reduction curve surrounding three punctures preserves a round or an almost-round curve.

The recent paper by González-Meneses and Wiest [23] presents a new algorithm for solving the reducibility problem in arbitrary braid groups, whose complexity is polynomial, both in braid length and braid index, modulo a conjecture regarding the speed of convergence of the cyclic sliding operation $\mathfrak{s}$ ([20]).

In the present paper we will partially prove this conjecture (see Theorem 2 below) and obtain our algorithm as a modification of the algorithm by González-Meneses and Wiest. Therefore we will always make use of the classical Garside structure since the work in [23] fits in the classical context. We refer to [23] for any definition regarding Garside-theoretical notions needed below.

In the braid group B_n endowed with the classical Garside structure, we define the length $|x|$ of a braid x as the minimal possible length of a word representing x whose letters are divisors of Δ and their inverses. We notice that for any braid x, the canonical length $\ell(x)$ (in the sense of [15]) satisfies the inequality $\ell(x) \leqslant |x|$.

We can now state our main result:

Theorem 1. *Let n be a positive integer. There exists an algorithm which decides the Nielsen-Thurston type of any given braid x with n strands and runs in time $O(|x|^3)$.*

We warn the reader that Theorem 1 is only an existence result. We will actually describe an algorithm which is not well-defined because we do not know explicitly the constant $C(n)$ in Theorem 2, which comes from Masur-Minsky's conjugacy bound [25]. Nevertheless, the existence of this constant is one of the keys for proving Theorem 1:

Theorem 2. *There exists a constant $C(n)$ (depending only on n) such that for any pseudo-Anosov n-strand braid $x \in SSS(x)$, the following holds: x has a rigid conjugate if and only if $\mathfrak{s}^{C(n)\cdot|x|}(x)$ is rigid.*

Theorem 2 gives a partial solution to a long-standing problem (see Conjecture 3.5 in [23]): in the pseudo-Anosov rigid case, starting from a super summit element, Theorem 2 guarantees that a rigid conjugate (or equivalently an element of the sliding circuits set) is found after only $C(n)\cdot|x|$ iterations of cyclic sliding (in other words, if a pA super summit braid has rigid conjugates, then the cyclic sliding operation converges towards one of them in linear time with respect to braid length).

The importance of the rigid case comes from the following result, which will play a crucial role in our proof of Theorem 1. It is due to Birman, Gebhardt and González-Meneses:

Theorem 3. [4]. *Let $x \in B_n$ be a pseudo-Anosov braid. There exists a positive integer $m < (\frac{n(n-1)}{2})^3$ such that x^m is conjugate to a rigid braid.*

In order to prepare the description of the algorithm promised in Theorem 1, we now recall the two following results from [23]:

Theorem 4. ([23], Theorem 5.16). *Let $x \in B_n$ be a non-periodic, reducible braid which is rigid. Then some essential reduction curve of x is round or almost-round. More precisely, there is some positive integer $k \leqslant n$ such that one of the following holds:*

(1) *x^k preserves a round essential curve,*
(2) *$\inf(x^k)$ and $\sup(x^k)$ are even and either $\Delta^{-\inf(x^k)}x^k$ or $x^{-k}\Delta^{\sup(x^k)}$ is a positive braid preserving an almost-round essential reduction curve whose interior strands do not cross.*

Theorem 5. ([23], Theorem 2.9). *There is an algorithm which decides whether a given positive braid x preserves an almost-round curve whose interior strands do not cross. Its complexity is $O(\ell(x)n^4)$.*

We are now ready to describe the algorithm promised in Theorem 1. It takes as input an n-braid x. The output is "periodic", "reducible" or "pseudo-Anosov".

1. If x^{n-1} or x^n is a power of Δ, return "periodic" and stop.
2. For $i = 1, \dots, (\frac{n(n-1)}{2})^3 - 1$ compute x^i. Iteratively apply cyclic sliding to x^i until the canonical length has not decreased during the $\frac{n(n-1)}{2} - 1$ last iterations. This computes $y_i \in SSS(x^i)$. Then compute $z_i = \mathfrak{s}^{C(n)\cdot|y_i|}(y_i)$. If none of the z_i's is rigid return "reducible" and stop. Else let j be such that z_j is rigid.
3. For $k = 1, \dots, n$, apply the algorithm in [1] to the braid z_j^k to test whether it preserves a round curve; apply the algorithm in Theorem 5 to both braids $\Delta^{-\inf(z_j^k)}z_j^k$ and $z_j^{-k}\Delta^{\sup(z_j^k)}$. If a round or an almost-round reduction curve is found, then return "reducible" and stop.
4. Return "pseudo-Anosov".

As mentioned above, we remark that this algorithm, and specifically Step 2, is not well-defined because the constant $C(n)$ is not explicitly known. In the next section, we will prove Theorem 2, show the correctness of the above algorithm and study its complexity.

2. Proofs of our results

We start with some more words about the braid length $|\cdot|$ defined above. Let us consider the length of n-braid words on the set of divisors of Δ and their inverses. By [16] and [14], there exists a unique decomposition of any braid of the form $a^{-1}b$, with a, b in B_n^+ and $a \wedge b = 1$. This is called the mixed canonical form. Moreover, if $a = a_1 \dots a_k$ and $b = b_1 \dots b_l$ are the left normal forms of a and b respectively (with possibly some factors equal to Δ), it is shown in [13] Lemma 3.1 that the word $a_k^{-1} \dots a_1^{-1} b_1 \dots b_l$ is a geodesic in the Cayley graph of B_n with respect to the

set of divisors of Δ. Therefore, the length $|x|$ of a braid x is the length of its mixed canonical form.

In order to prove Theorem 2, we need to combine two important results. The first one is a general fact due to Masur and Minsky about the length of conjugators in mapping class groups. Although the range of surfaces considered by Masur and Minsky is much broader, only the $(n+1)$-times punctured sphere $\mathbb{S}_{n+1}$ $(n \geqslant 2)$ is relevant for our purposes, so we state their result in this special case:

Theorem 6. ([25], Theorem 7.2). *Let $\mathcal{G}$ be any generating set of the modular group $\mathcal{MCG}(\mathbb{S}_{n+1})$. There exists a constant $\gamma(\mathcal{G})$, depending only on $\mathcal{G}$, such that any pair of conjugate pseudo-Anosov mapping classes can be related by a conjugating element w satisfying*
$$|w|_{\mathcal{G}} \leqslant \gamma(\mathcal{G})(|x|_{\mathcal{G}} + |y|_{\mathcal{G}}),$$
(where $|\cdot|_{\mathcal{G}}$ denotes the word length with respect to the chosen generating set $\mathcal{G}$).

We aim at an analogous result for braids, namely we want to show:

Proposition 7. *There exists a constant $c(n)$, depending only on n such that any pair of conjugate pseudo-Anosov n-braids can be related by a conjugating element w satisfying*
$$|w| \leqslant c(n)(|x| + |y|).$$

Proof. We recall that $B_n/\left\langle\Delta^2\right\rangle$ can be seen as the mapping class group of an n-times punctured closed disk (with boundary fixed setwise). For a braid x in B_n, let us denote by $\hat{x}$ its image in the quotient $B_n/\left\langle\Delta^2\right\rangle$. The set of simples in the classical Garside structure of B_n induces a word length on the quotient $B_n/\left\langle\Delta^2\right\rangle$ which we denote by $||\cdot||$ (notice that for any braid x, $||\hat{x}|| \leqslant |x|$). Collapsing the boundary of the n-times punctured closed disk to a puncture in the sphere $\mathbb{S}_{n+1}$, we can view $B_n/\left\langle\Delta^2\right\rangle$ as the finite index subgroup of $\mathcal{MCG}(\mathbb{S}_{n+1})$ consisting of the mapping classes which fix the $(n+1)$st puncture. The group $\mathcal{MCG}(\mathbb{S}_{n+1})$ is equipped with the generating set $\mathcal{G}_n$ consisting of the Garside generators of B_n (or more precisely their image in the quotient $B_n/\left\langle\Delta^2\right\rangle$) together with a rotation by an angle of $\frac{2\pi}{n+1}$ (notice that for any $u \in B_n/\left\langle\Delta^2\right\rangle$, we have $|u|_{\mathcal{G}_n} \leqslant ||u||$). In this setting, the inclusion of the finite index subgroup $B_n/\left\langle\Delta^2\right\rangle \hookrightarrow \mathcal{MCG}(\mathbb{S}_{n+1})$ is a Lipschitz embedding, i.e. there exists a constant $\kappa(n)$ such that for any $u \in B_n/\left\langle\Delta^2\right\rangle$, the inequality $||u|| \leqslant \kappa(n)|u|_{\mathcal{G}_n}$ holds.

Now, given a pair of conjugate pseudo-Anosov n-braids x and y, we know a conjugating element between $\hat{x}$ and $\hat{y}$, say υ in the quotient $B_n/\left\langle\Delta^2\right\rangle$. Masur-Minsky's proof of Theorem 6 constructs a "short" conjugating element υ' between $\hat{x}$ and $\hat{y}$ in $\mathcal{MCG}(\mathbb{S}_{n+1})$. The mapping class υ' is the product $\hat{x}^m\upsilon$, for some integer m and therefore υ' actually belongs to the subgroup $B_n/\left\langle\Delta^2\right\rangle$ of $\mathcal{MCG}(\mathbb{S}_{n+1})$. Moreover,
$$|\upsilon'|_{\mathcal{G}_n} \leqslant \gamma(\mathcal{G}_n)(|\hat{x}|_{\mathcal{G}_n} + |\hat{y}|_{\mathcal{G}_n}) \leqslant \gamma(\mathcal{G}_n)(||\hat{x}|| + ||\hat{y}||)$$
and we get
$$||\upsilon'|| \leqslant \kappa(n)\gamma(\mathcal{G}_n)(||\hat{x}|| + ||\hat{y}||).$$

Finally, as $\left\langle\Delta^2\right\rangle$ is the center of B_n, and because a braid x conjugate to y cannot be conjugate to $\Delta^{2k}y$ for $k \neq 0$, any lifting of υ' in B_n conjugates x to y and we

can choose one, say w, so that $|w| = ||v'||$. Therefore, taking $c(n) = \kappa(n)\gamma(\mathcal{G}_n)$ achieves the proof of Proposition 7. □

The next step towards Theorem 2 is a general fact about Garside groups. It explains that if a super summit element has a rigid conjugate, then iterated cyclic sliding is the shortest way of obtaining such a rigid conjugate.

Theorem 8. [20]. *Let $x \in B_n$ and assume that x is conjugate to a rigid braid.*

(1) *There exists a unique positive braid $f(x)$ such that $x^{f(x)}$ is rigid and $f(x) \leqslant g$ for any positive braid g such that x^g is rigid.*
(2) *If $y \in SSS(x)$, then (unless y is already rigid) there exists some positive integer k such that $f(y) = \prod_{i=1}^{k} \mathfrak{p}(\mathfrak{s}^{i-1}(y))$. That is, $f(y)$ is the product of the k conjugating simple elements involved when applying k iterations of cyclic sliding to y.*

Now, the proof of Theorem 2 is just a combination of both of the previous results.

Proof of Theorem 2. Let x be a pseudo-Anosov n-strand braid such that $x \in SSS(x)$. Let us assume that x has a rigid conjugate z. By Proposition 7, there exists $w \in B_n$ such that $z = x^w$ and $|w| \leqslant c(n)(|x| + |z|)$. Since $x, z \in SSS(x)$, we have $|x| = |z|$. Let r be the number of negative factors in the mixed canonical form of w. If r is even, then $w' = \Delta^r w$ is a positive braid conjugating x to z (recall that Δ^2 is central). Otherwise r is odd and $w' = \Delta^{r+1} w$ does the same job. In either case, we get a positive braid w' conjugating x to z with $|w'| \leqslant |w| + 1 \leqslant (2c(n) + 1)|x|$ (we may assume that $|x| \geqslant 1$).

Let k and $f(x) = \prod_{i=1}^{k} \mathfrak{p}(\mathfrak{s}^{i-1}(x))$ be as in Theorem 8. Then $f(x) \leqslant w'$. It follows that $|f(x)| \leqslant |w'|$. Let $q = \frac{n(n-1)}{2}$ be the length of Δ with respect to the atoms. As the braid $f(x)$ is a product of k simple elements, we have $\frac{k}{q} \leqslant |f(x)|$. It finally follows that $k \leqslant q \cdot (2c(n) + 1)|x|$. Thus taking $C(n) = \frac{n(n-1)}{2} \cdot (2c(n) + 1)$ (which depends only on n), we have shown the following: x has a rigid conjugate if and only if $\mathfrak{s}^{C(n)\cdot|x|}(x)$ is a rigid braid (notice that $\mathfrak{s}^m(z) = z$ for any rigid braid z and any integer $m \in \mathbb{N}$). □

We notice that Theorem 2 can be shown as well in the dual setting but we will not need this. We now turn to the proof of Theorem 1, showing the correctness of the algorithm in the Introduction and studying the complexity of each step.

Proof of Theorem 1. The correctness of Step 1 is shown in [6]. This step just consists in a computation of left normal form; therefore it takes time $O(\ell(x)^2)$ for any fixed n, according to [16].

Let us prove that Step 2 is correct. First, it follows from the results in [8] and [20] that starting from any n-braid x, then either x is an element of $SSS(x)$ or iteratively applying the cyclic sliding operation $(\frac{n(n-1)}{2} - 1)$ times to x decreases the canonical length. Therefore for each i, the braid y_i is an element of $SSS(x^i)$. Then if x is a pseudo-Anosov braid, by Theorem 3, at least one of the braids x^i (and therefore y_i) is pseudo-Anosov with a rigid conjugate and by Theorem 2 at least one of the braids z_i is rigid.

Let us calculate the complexity of Step 2. We recall that each instance of cyclic sliding has quadratic complexity with respect to the braid length for any given braid index (see [21], Theorem 4.4). Therefore for any $i = 1, \dots, (\frac{n(n-1)}{2})^3 - 1$, the complexity of computing y_i (which requires at most $(\ell(x^i)-1)\cdot(\frac{n(n-1)}{2}-1)$ iterations of cyclic sliding) is cubic with respect to the braid length whenever n is fixed. The same is true for the computation of z_i from y_i which requires $C(n)|y_i| \leqslant C(n)i|x|$ iterations of cyclic sliding.

The validity of Step 3 follows from Theorem 4. This step consists in applying the algorithm in [1] to at most n braids of length at most $nj|x|$ and the algorithm of Theorem 5 to at most $2n$ braids of length at most $nj|x|$. Both of these algorithms work in linear time with respect to the length so that Step 3 is linear with respect to $|x|$. □

We notice that the present algorithm does not always yield the knowledge of reduction curves for reducible elements (actually this failure happens when reducibility is detected at Step 2). Thus, in view of the program in [4], [5], [6], writing an algorithm for solving the conjugacy problem in braid groups in polynomial time requires the following:

(i) find explicitly the constant $C(n)$ to make the algorithm in Theorem 1 explicit. This amounts to bounding explicitly the required number of cyclic slidings to obtain (if it exists) a rigid conjugate from a pseudo-Anosov super summit element (see Theorem 2); alternatively this rests on the knowledge of an explicit value for Masur-Minsky's constant $c(n)$ (see Proposition 7),
(ii) find reduction curves of a braid, in polynomial time, whenever the braid is known to be reducible,
(iii) find a polynomial bound on the number of rigid braids in a given pA conjugacy class.

We finish with a discussion of the special case of the four-strand braid group B_4. If we want to decide the Nielsen-Thurston type of a given 4-braid, the algorithm in [11] should rather be used instead of the present one because it is implementable and it finds explicitly the reduction curves whenever they exist (in polynomial time). Using the Birman-Ko-Lee structure of B_4, the author together with Bert Wiest show in a forthcoming paper [10] the existence of a bound as in (iii) (which depends on Masur-Minsky's constant $c(4)$, see Proposition 7). Unfortunately, they do not know yet how to make explicit the constant $c(4)$ (nor $C(4)$), so that the cardinality of the ultra summit set of a pseudo-Anosov rigid 4-braid is not explicitly known. Nevertheless [10] presents a polynomial-time algorithm for solving the conjugacy problem in B_4.

Acknowledgements. The author thanks Jin Tao for her help with Proposition 7 and Juan González-Meneses for useful comments on an earlier version of that work. His gratefulness also goes to Bert Wiest for many inspiring discussions and careful readings of the manuscript.

References

[1] D. Benardete, M. Gutierrez, Z. Nitecki, *A combinatorial approach to reducibility of mapping classes*, Mapping class groups and moduli spaces of Riemann surfaces (Göttingen, 1991/Seattle, WA, 1991), 1-31, Contemp. Math., 150, Amer. Math. Soc., Providence, RI, 1993.

[2] D. Benardete, M. Gutierrez, Z. Nitecki, *Braids and the Nielsen-Thurston classification*, J. Knot Theory Ramifications, 4 (1995), 549-618.

[3] M. Bestvina, M. Handel, *Train-tracks for surface homeomorphisms*, Topology 34 (1995), no. 1, 109-140.

[4] J. Birman,V. Gebhardt, J. González-Meneses, *Conjugacy in Garside Groups I: Cycling, Powers and Rigidity*, Groups Geom. Dyn. 1 (2007), no. 3, 221-279.

[5] J. Birman,V. Gebhardt, J. González-Meneses, *Conjugacy in Garside Groups II: Structure of the ultra summit set*, Groups Geom. Dyn. 2 (1), (2008), 16-31.

[6] J. Birman, V. Gebhardt, J. González-Meneses, *Conjugacy in Garside groups III: Periodic braids*, J. Algebra 316 (2), (2007), 746-776.

[7] J. Birman, K.-H. Ko, S.-J. Lee, *A new approach to the word and conjugacy problems in the braid groups*, Adv. Math. 139 (2) (1998) 322-353.

[8] J. Birman, K.-H. Ko, S.-J. Lee, *The infimum, supremum, and geodesic length of a braid conjugacy class*, Adv. Math. 164 (2001) 41-56.

[9] M. Calvez, *Dual Garside structure and reducibility of braids*, preprint arXiv:1105.3675v1

[10] M. Calvez, B. Wiest, *The conjugacy problem in the four-strand braid group*, in preparation.

[11] M. Calvez, B. Wiest, *Fast algorithmic Nielsen-Thurston classification of four-strand braids*, arXiv:1004.0067v3, to appear in J. Knot Theory Ramifications.

[12] A. Casson, S. Bleiler, *Automorphisms of surfaces after Nielsen and Thurston*, LMS Student Texts, 9. Cambridge University Press, Cambridge, 1988.

[13] R. Charney, J. Meier, *The language of geodesics for Garside groups*, Math. Z. 248 (2004), no. 3, 495-509.

[14] P. Dehornoy, *Groupes de Garside*, Ann. Sci. École Norm. Sup. (4) 35 (2002), no. 2, 267-306.

[15] E. ElRifai, H. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford. Ser. (2) 45 (1994), no. 180, 479-497.

[16] D. B. A. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson, W. Thurston, *Word processing in groups*, Jones and Bartlett Publishers, Boston, MA, 1992.

[17] B. Farb, D. Margalit, *A primer on mapping class groups*, http://www.math. utah.edu/ margalit/primer/

[18] A. Fathi, F. Laudenbach, V. Poenaru, *Travaux de Thurston sur les surfaces*, Astérisque 66-67, SMF 1991/1979.

[19] F. Garside, *The braid groups and other groups*, Quart. J. Math. Oxford Ser. (2) 20 (1969), 235-254.

[20] V. Gebhardt, J. González-Meneses, *The cyclic sliding operation in Garside groups*, Math. Z. 265 (1), (2010), 85-114.

[21] V. Gebhardt, J. González-Meneses, *Solving the conjugacy problem in Garside groups by cyclic sliding*, Journal of Symbolic Computation 45 (6) (2010), 629-656.

[22] J. González-Meneses, *On reduction curves and Garside properties of braids*, Contemp. Math. 538 (2011), 227-244.

[23] J. González-Meneses, B. Wiest, *Reducible braids and Garside theory*, arXiv:1008.0238 to appear in Alg. Geom. Top.

[24] E.-K. Lee, S.-J. Lee, *A Garside-theoretic approach to the reducibility problem in braid groups*, J. Algebra 320 (2008), no. 2, 783-820.

[25] H. Masur, Y. Minsky, *Geometry of the complex of curves. II. Hierarchical structure*, Geom. Funct. Anal. 10 (2000), no. 4, 902-974.

[26] M.V. Prasolov, *Small braids with large ultra summit set*, Mat. Zametki 89 (4) (2011), 577-588.

Matthieu Calvez, IRMAR (UMR 6625 du CNRS), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

E-mail address: matthieu.calvez@univ-rennes1.fr